Project Supervisor: Dr M. Kuhn
Director of Studies: Dr T. Sauerwald
Overseers: Dr R. Mantiuk and Dr I. Wassell

Benjamin O'Neill
Emmanuel College
bo271@cam.ac.uk
31 January 2018

Progress Report:

Efficient Asymmetric Cryptography for RFID Access Control

Project mostly on schedule:

According to the original schedule, I should now have finished one or two of the optional project extensions, but I am only now nearing completion of the core project.

The core implementation took longer than anticipated due to the particularly arduous debugging process, and various complications that arose during the implementation of the core project, often as a result of incompatibilities and library deficiencies, requiring more work to compensate. I am on track to finish the core project on time, but the extensions will be disregarded for now.

Progress towards success criteria:

1. Card authentication time should be no longer than a second:
   Currently too high, over 3 seconds. Will be looking into improvements to decrease this. The OPACITY protocol defines an optimised version involving caching information from previous interactions, which would significantly improve authentication time, but the implementation of this is not yet complete.

2. Access rights of a card should be revocable without access to the card itself:
   This is done by simply removing the card ID from the door's list of allowed cards.

3. Allow for unlimited number of doors with different access privileges:
   This is possible, though in theory the optimized implementation would eventually have to discard cached previous interactions, reverting to the basic case.

4. The system should be secure:
   Full security analysis not yet carried out, but the protocol itself is considered secure.

5. The introduction cost should not exceed that of a typical smartcard system:
   In bulk orders, smartcards cost under £4 each. The implementation doesn't require terminals with Secure Authentication Modules (SAMs), keeping the cost down.

Work accomplished:

Learned about smartcards and the development process for them, built a number of small programs for smartcards prior to beginning the main project.
Explored different smartcard versions and their respected supported library functionality.
Implemented 'OPACITY' protocol. In the process, implemented auxiliary cryptographic and modular arithmetic functions not supported by the library version.
Key issuing and authentication is performed by portable Python code that interfaces with the smartcard applet.